Riot Offensive Security

Rules of Engagement

Client **Name**
Date

Executive Summary

This Rules of Engagement (ROE) states that Client Name gives approval, authorization, and has discussed the necessary steps to execute the engagement. Signing this ROE document constitutes acknowledgement and approval of the customer, system owner, and client authorities in execution of this engagement against the discussed target.

Riot Offensive Security will preform penetration testing against the requested target with the objective to identify service vunerabilities and provide mitigation strategies, penetration testing encompasses a series of steps including:

- Reconnaissance, Riot Offensive Security will use information provided to us and begin building a client profile, verifying target authenicity before taking the next steps.
- Scanning & Enumeration, Riot Offensive Security may use tools & scripts to create network mappings, identify vunerabilities, or gather deeper information on the target.
- Gaining Access, in the event a vunerability is found, Riot Offensive Security may use tools & scripts to prove the validitiy and threat of found vunerability.

- Maintaining Access, in the event a vunerability is attacked, Riot Offensive Security may use tools & scripts to prove persistence in an attack.
- Covering Tracks, Riot Offensive Security takes cleanup seriously, our team assures we will be diligenint in removal of any tools & scripts that may have been placed on the target and restore any modifications back to the original state.

Explicit Restrictions:

- DoS (Denial of Service)

Authorized Target Space:

- Enter Targets
-

Activities:

- Reconnaissance
- Scanning & Enumerating
- Access
- Mitigation

TABLE OF CONTENTS

Section Page

- RULES OF ENGAGEMENT INTRODUCTION
- Purpose

To establish the responsibilities, relationships, and guidelines between Riot Offensive Security, Client Name, Client Name Systems, and Client Name Authorities, for conducting an engagement on services relating to Target Name hereafter referred to as “target of engagement”.

- References:
  - PIA …
  - HIPAA …
  - ISO …

- Scope

This agreement is applicable to Client Name for the receipt of Riot Offensive Security activities. This document will establish the guidelines, limitations, and restrictions for conducting a Riot Offensive Security engagement.

- Definitions

Penetration Testing: Security testing in which evaluators mimic real-world attacks to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data with the same tools and techniques used by actual attackers.

Vulnerability Scanning: A technique used to identify hosts/host attributes and associated vulnerabilities.

Vulnerability: Weakness in an information system, or in system security procedures, internal controls, or implementation, that could be exploited or triggered by a threat source.

Target Vulnerability Validation Techniques: Also known as an "attack" these are security testing techniques that corroborate the existence of vulnerabilities. They include password cracking, remote access testing, penetration testing, social engineering, and physical security testing.

Tools: Tools are defined by programs and codes designed for vunerability discovery & validation, these tools may include, web proxies, scanners and codes, these tools may be intrusive or may have negative affects against some systems.

- RULES OF ENGAGEMENT AND SUPPORT AGREEMENT:

  - Riot Offensive Security has agreed to conduct a security engagement. This document provides the ground rules for planning, executing and reporting the engagement.

  - The following systems, networks and/or assets will be included:

    - Target Name/IP Addresses
    - Target Name/IP Addresses
    - Additional systems, networks, or websites may be requested by client
    - Off limits IP/Hosts lists are provided in Appendix A. These list should only include IPs/hosts within the network that are not part of the engagement.
    - Riot Offensive Security will attempt to gain access to the target of engagement.
    - Riot Offensive Security activities are limited to the target of engagement.
    - Riot Offensive Security efforts will be coordinated with Client Name (Best POC) for the duration of the engagement. Riot Offensive Security will target only provided hosts and internet protocol (IP) addresses.

  - The engagement objective is to breach administrator level on target of engagement. This means Riot Offensive Security may take any non-restricted method to reach the desired objective.
    - Riot Offensive Security, will utilize an open network. An open network is defined as a network with access to the internet.
    - Riot Offensive Security operations require the use of exploitation and attack tools and techniques. All tools employed by Riot Offensive Security have been extensively tested by the team to ensure they are non-destructive and are under positive control when employed.
    - Riot Offensive Security systems contain exploit tools, code, and technical references, which are not to be viewed, distributed or evaluated by external organizations.
    - Riot Offensive Security methods may be intrusive, but will not intentionally disrupt services outside the authorizations of Rules of Engagement and should not be destructive.

- Services will be terminated if information is gathered pertaining to an actual intrusion. Riot Offensive Security is responsible for informing Client Name (Best POC) if an actual intrusion is discovered. Client Name will report the actual intrusion to the appropriate representative, along with any substantiating information regarding the detected intrusion.

- Riot Offensive Security may provide updates as follows:
    - Riot Offensive Security will contact the client in the event another intrusion is detected.
    - Riot Offensive Security will contact the client in the event a service breaks, or becomes unavalible.
    - Riot Offensive Security will contact the client in the event a method to administrator is discovered.
    - Riot Offensive Security may contact you with general update informing the client how things are looking.
    - Riot Offensive Security will contact you at the end of the engagement.

- <u>Client Name will:</u>

    - Provide IP address range(s) for desired target(s) of engagement.
    - Provide domain and subdomains for desired target(s) of engagement.
    - Coordinate support of Riot Offensive Security activities, with the appropriate stakeholders.
    - Provide contact information (i.e., names, titles, phone & email address) to the signatories of this document.

- <u>Sensitive information reporting:</u>

    - Incidental discovery of information that relates to serious crimes such as sabotage, threats, or plans to commit offenses that threaten a life or could cause significant damage to or loss of customer property, and which does not present an immediate risk, will be reported to the applicable local authorities for action.
    - Riot Offensive Security reporting is otherwise conducted in a way that does not attribute information or particular activity to an individual.
    - Riot Offensive Security activities may not be conducted in support of law enforcement or criminal investigation purposes.

- Cease operations process:

  - Riot Offensive Security will suspend activity upon detection of computer anomalies that could potentially be unauthorized intrusions into target of environment networks, until the appropriate reporting has taken place.
  - All engagement activities operate under the direction of the Engagement Director, who may alter or cease activities as necessary.

- Information usage:

  - Riot Offensive Security will not intentionally compromise Privacy of Information Act (PIA), medical, justice, worship or religious pursuit, or any other protected or privileged information. If a compromise does occur, it will be handled through normal procedures. The proper security personnel will be notified immediately.
  - Riot Offensive Security is authorized to exploit files, email, and/or message traffic stored on the network, as well as communications transiting the network for analysis specifically related to the accomplishment of their objectives. (e.g., identifying user ID's, passwords and/or network IP addresses in order to gain further access).
  - Riot Offensive Security will not intentionally modify or delete any operational user data, or conduct any Denial of Service attacks. Riot Offensive Security will not otherwise intentionally degrade or disrupt normal operations of the targeted systems.
  - Riot Offensive Security reporting is conducted in a way that does not attribute information or particular activity, to a specific individual.

- Deconfliction process:

  - All detected information assurance incidents, whether real-world or alleged Riot Offensive Security activity, should immediately be reported using normal incident reporting processes.
  - Any Client Name POC may contact any Riot Offensive Security's POC to determine if discovered activities are the result of Riot Offensive Security.

- Deliverables:

- Riot Offensive Security will provide an engagement summary presentation for the target of engagement representatives at the completion of the engagement.
- Riot Offensive Security will provide a written summary of the engagement results to the Client Name (Best POC) within 14-30 days following completion of the test.

- ROE Provisions

The following additional provisions apply to this memorandum:

- All operations will be conducted within guidelines established by applicable policy, regulations and laws.

- All contact with computer networks/subnets will be from within Riot Offensive Security or target of engagement environment.

- During the engagement, any deviations from these ROE must be mutually agreed to and approved in writing by the senior representatives for Riot Offensive Security, Client Name and any stakeholders required for engagement execution.

- Requirements, Restrictions, and Authority
  - Riot Offensive Security will:

    - Provide the appropriate support and input for the planning of the engagement.
    - Coordinate engagement approval and support via this Rules of Engagement (ROE).
    - Inform target of engagement POCs of all team requirements (logistics, administrative, etc.).
    - Coordinate team personnel and administrative issues/concerns with Client Name (Best POC).
    - Provide contact information (i.e. names, job titles, phone & email address) to the client representatives.
    - Escalate problems and issues to the appropriate representatives.
    - Upload, where appropriate, indicators on systems to demonstrate a compromised state.
    - When necessary, add/modify/disable accounts (not delete them) on compromised systems.
    - Conduct exploitation with the intent of emulating threat techniques, tactics and procedures.

- May view/read or modify personal data files, PII, or emails.
- NOT use unapproved tools.
- NOT damage systems or networks.
- NOT conduct denial of service (DOS), except as explicitly approved.

- Ground Rules

This section identifies specific rules associated with the execution of this event.

- Network Operations
  - All systems outside the IP ranges provided under separate cover are off limits
  - Riot Offensive Security will abide by targeting rules as defined in Appendix A

- Resolution of Issues/Points of Contact (POC)

Any issues that may develop, which are not covered by this ROE, will be resolved mutually with all stakeholders.

Client Name(Best POC):

- Name:
- Title:
- Email:

- AUTHORIZATION

This agreement becomes effective upon the date of the last approving official's signature.

Termination of this agreement can be directed by any of the stakeholders listed in this document at any time by giving notice in writing to the non-terminating parties. This agreement can only be modified by mutual written consent of the signatories. Changes must be coordinated by means of an exchange of memoranda between the signatories. This agreement will undergo a review in its entirety with each modification request or by the request of either party after giving notice in writing at least 7 days prior to the review.

- APPROVAL

The signatures below denote that all parties have read and agree to this Memorandum of Agreement.

_____	_____
(NAME)	(NAME)
Lead Security Tester	Chief Information Officer
Riot Offensive Security	Client Name
_____	_____
(Date)	(Date)
_____	_____
(NAME)	(NAME)
Security Researcher	Chief Executive Officer
Riot Offensive Security	Client Name
_____	_____
(Date)	(Date)

- APPENDIX A – TARGET ENVIRONMENT

List of assets, systems and data

Restricted IP Addresses:

- List any restricted ip addresses here
-

Authorized IP Space:

- Autorized IP here

-

Restricted Hosts:

- List any restricted hosts here
-

Authorized Hosts:

- Authorized Hosts here
-

- APPENDIX B - POINTS OF CONTACT

Riot Offensive Security Team

Engagement Director(Emergancy Contact):

- Name: Lead Tester Name here
- Title: Lead Security Tester
- Email: riotsecurity@proton.me

Engagement Researcher

- Name: Security Researcher Name here
- Title: Lead Security Researcher
- Email riotsecurity@proton.me

- APPENDIX C – RIOT OFFENSIVE SECURITY METHODOLOGY

Get-In:

- Reconnaissance
    - Perform Open Source Intelligence (OSINT) against the target
    - Search using open unauthenticated sources
    - Target web sites
    - Social Media
    - Search engines

        - Public Code repositories
- Enumeration
    - Identify/confirm external assets
    - Perform reverse DNS scan to identify registered hosts
    - Preform vunerability scan
    - Preform subdomain lookups
    - Identify URLs and external touch points from scan and OSINT
    - Web presence evaluation
    - Browse as a normal user through a web proxy to capture intelligence and understanding
    - Identify known vulnerabilities and vulnerable conditions
- Exploitation
    - Attempt to exploit targets based on current knowledge
    - Perform situational awareness on target
    - Attempt Local Privilege Elevation
    - Attempt Domain or other system level Privilege Elevation

Stay-In:

- Post Exploitation
    - Identify domain user/groups/memberships
    - Identify IP space
    - Identify file shares
    - Establish persistence
    - Use persistence plan to place agents on target systems
    - Move Laterally
- Continued Lateral Movement
- Continued Enumeration

Act:

- Impact
    - List impacts caused

- APPENDIX D – ENGAGEMENT OBJECTIVES

Objective defines the ultimate end goal of the engagement as defined by Client Name.

Objective 1:

- List Client engagement objectives here